U.S. Department of State
Privacy Impact Assessment Summary

TITLE: Privacy Impact Assessment for Public Key Infrastructure/Biometric Logical Access Development and Execution (PKI/BLADE)
Date: 2007

I. Describe the information to be collected (e.g., nature and source). Be sure to include any information in an identifiable form, e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc).

Currently, no identifiable information is being collected or stored on members of the public. All employees of the Department of State who use the Departments Public Key Infrastructure (PKI) are required to apply for certificates. The Department anticipates that members of the public (e.g., family members) will require PKI certificates to access Department resources abroad in the very near future.

Should members of the public apply for certificates, they will be required to provide their name, email address, a physical address, phone number, and the numbers of identification with which they identify themselves. This may include driver's license number, passport number, or other government identification.

II. Why is the information being collected (e.g., to determine eligibility)?

Information is required to be collected in order to issue certificates for the Department's Public Key Infrastructure per the Federal Bridge Certificate Authority.

III. How will the information be used (e.g., to verify existing data)?

To document an individual's identity.

IV. Will you share the information with others (e.g., another agency for a programmatic purpose)? If yes, list the entities.

The information will not be shared, per se. The individual's name and email address is part of the information contained in a certificate. Any use of the certificate, by definition, shares the name. (There is no such thing as anonymity when using a PKI; hence, the requirement to identify one's self.)

V. Describe what opportunities individuals have been given to decline to provide information or to consent to particular use of the information (e.g., whether individual may withhold permission for a particular use).

Should a member of the public not wish to have a certificate, that is their option. Should the use of certificates be required to access certain Department resources, then a failure to apply for and receive such certificates would deny them access to any system requiring it.

VI. How will the information be secured (e.g., administrative and technological controls)?

The application for a certificate will be maintained in a secured area within the Department of State for no less than 20 years, 6 months. The files, which are originally executed in a paper format, will ultimately be converted to digital format, and will be retained for no less than that period of time on limited access computer systems. The name and email address of the individual will be available on public certificates, as that is part of the individual's identify.

VII. How will the data be retrieved (e.g., will it be retrieved by a personal identifier such as name, social security number, address, telephone number or some other identifier that is unique to an individual)?

Only the individual's name and email address are publicly retrievable, much the same as that information is retrievable today through the Department's e-mail Global Access List (GAL). Application forms will be retrievable through any of the fields that are required for the application for a certificate; however, only authorized personnel will have access to the database in which applications will be stored.